Task 3.2 GISRA/FISMA Reporting

Task Overview

FSA, as part of the Department Of Education, must submit GISRA/FISMA* reports annually to OMB. This process requires the completion of Self-Assessments and the creation of an agency-level report. To support this initiative, BearingPoint will create and conduct specialized Self-Assessment training courses for FSA employees and their contractor counterparts. Additionally, we will coordinate the submission of the Self-Assessments to the Department and implement a tracking program to measure performance against FSA's 2002 baseline.

Soon after the annual reports are submitted, OMB requires the creation of Plans of Actions and Milestones (POA&Ms) to document and track the remediation of weaknesses described in the annual report. With the POA&Ms established OMB requires quarterly reports (submitted by the Department) on the progress of all POA&M actions. To support this initiative we will work with the OCIO to track FSA POA&M actions, meet and work with the SSO's, system managers, and the contractors for FSA systems to make sure their actions are completed on time and recorded properly.

Task Details Period 1

We began supporting FSA's Security and Privacy team in January 2003, after the completion and submission of their 2002 annual report and POA&M actions.

The first steps in support of the security and privacy team was to assist FSA SSO's with updating and validating their Inventory Worksheet and CIP Survey. This was done for all FSA MA's, GSS's, and Applications. Once the SSO's reviewed, verified, and updated the information on the worksheet and Survey, we reviewed the information and submitted the updated FSA inventory (all GSS's and MA's) for review and submission to the Department (a biannual requirement). The information from the survey and worksheet also determined the Tier of the system (based on mission criticality, confidentiality, integrity, and availability of the system). We updated the FSA System Tier Identification Sheet also.

Our next area of support was the tracking and monitoring of POA&M action items that will be reported by OCIO to OMB in the quarterly report due April 1, 2003. We attended weekly meetings with OCIO to ensure consistency between our status information OCIO's. This included information on FSA items that were closed, still open, and late. This review is accomplished on a weekly basis (2-3 times a week) by checking the public folders for each tier 3 and 4 system and checking their POA&M sheets to see their status.

Since quite a few action items were late we determined the need to meet with each system on an individual basis to discuss in detail their status. Members of the Security and Privacy team, SMs, SSOs and contractors (as necessary) attended the meetings.

At the meetings we also distributed checklists for the systems to review their Disaster Recovery/Continuity of Support Plan and their Change Management Plan. We also requested (because of a new Department requirement) that for each action item that was late (or would be late by February 28, 2003) that they create steps and dates that would lead to the completion of the outstanding actions.

Task Details Period 2

Period 2 of our task order began by working with the FSA systems that still had overdue (past the February 28, 2003 deadline) action items on their POA&Ms. We provided them a template to fill in information about the steps they would take to get the actions closed and the dates they expected to complete them. We then gathered their explanations and submitted them to ED/OCIO for review. We then worked with the Department to make sure the actions we were reporting were consistent with those they still considered overdue. We continued to provide the Department with updates throughout March and had them remove any systems from the overdue list that had completed their actions before the April quarterly report was submitted to OMB. Due to the efforts of the Security and Privacy Team we were able to remove all but eight items from the overdue list.

We continued tracking and monitoring POA&M action items that will be due on May 5, 2003 as required by the Department and that will be reported by OCIO to OMB in the quarterly report due August 2003. We attended meetings with OCIO to ensure consistency between our status information and OCIO's. This included information on FSA items that were closed, still open, and still late. We contacted and reminded the SSO's of all the actions they have yet to complete that will be considered late after May 5. We continue to review their progress on a weekly basis (2-3 times a week) by checking the public folders for each tier 3 and 4 system and checking their POA&M sheets to see their status.

In another area of the task and in preparation for helping FSA systems fill out and compete their 2003 Self-Assessments for FISMA, we created an informational PowerPoint briefing that we provided to all the attendees of the April 1, 2003 SSO Security Training Meeting.

The briefing explained at a high level, that FISMA replaced GISRA and that there are some noticeable differences between the two acts. We notified them that the Self-Assessments would more-than-likely still be required and that they will need to complete them by May 30, 2003. This date is tentative due to the fact that OMB still has not released guidance as to how to comply with FISMA. It is expected that OMB will release this guidance at the beginning of May. We will then provide training to the SSO's and their contractor personnel. We also notified them in the briefing that FSA will begin to track their level status on the Self-Assessments from year to year and expects to see progress.

Task Details Period 3

Period 3 of our task order began by working with the FSA systems that still had overdue (past the May 5, 2003 deadline) action items on their POA&Ms. We provided them a template to fill in information about the steps they would take to get the actions closed and the dates they expected to complete them. We then gathered their explanations and submitted them to ED/OCIO for review. We then worked with the Department to make sure the actions we were reporting were consistent with those they still considered overdue. We continued to provide the Department with updates throughout May and June and had them remove any systems from the overdue list that had completed their actions before the July quarterly report was submitted to OMB. Due to the efforts of the Security and Privacy Team we were able to remove all but one item from the overdue list.

We then turned our attention to the Self-Assessment surveys. Because the Department had a new format for their surveys, we reviewed the changes and briefed the SSOs and their contractors at our monthly SSO meeting in June. We went over the changes with them and told them how they should be filled out. The Department is pre-populating the survey with last year's answers so we told the SSOs and contractors to review their answers and make any updates to the form. As of the printing of this deliverable ED/OCIO has still not provided us the pre-populated forms to give to the systems

Task Details Period 4

Period 4 of our task order began with sending out the pre-populated Self-Assessments to all FSA Major Applications and General Support Systems. We then worked with the SSOs and Contractors to update any changes to last years information over the phone, in-person and by email. Reminders of the date they were due were sent out on a weekly basis. Once a system submitted their Self-Assessments we reviewed them for any glaring errors/omissions and sent them back to those systems that had made errors/omissions. Once they were all received, reviewed, and corrected we submitted them to the Department.

Our next area of focus was the CIP survey's sent out by the Department. The survey was updated/changed by the Department this year and included additional questions. Those questions that remained from last year's surveys were pre-populated. The CIP Surveys were then sent out to all FSA MAs and GSSs. We sent out numerous email reminders to the SSOs reminding them to complete the surveys by the submission deadline. Some of the questions on the survey were vague so we requested clarification from the Department and passed that information on to the SSOs to help them complete the surveys. All CIP Surveys were then gathered and reviewed for completeness. We then gave them scores (per the Departments scoring methodology) and forwarded all completed surveys to the Department. A Summary Results Table was created showing the various systems and their numerical results of each section of the survey. We continue to work with the Department and FSA systems in correcting overlooked errors on FSA CIP submissions and in gathering surveys for those systems that submitted their surveys late.

Even though Certification & Accreditation is in a separate task area, the tracking of the Pre-Certification Corrective Action Plans (CAP) was handled under this task and during this deliverable period. After BAH reviewed all of FSA's systems security documents they sent us the findings and suggested steps for remediation for each of the systems. We forwarded these findings and their recommendations for remediation to the appropriate SSOs. We required each SSO to create a CAP for the systems under their control and to provide tentative completion dates for each of the findings. We assisted in monitoring and tracking all of these Pre-Certification CAPs. This entailed providing updates on completion and delinquency and working with the SSOs to help them meet the deadlines. As part of the tracking process we created a simple MS Access database to allow the security team to easily track, find and present data. All Pre-Cert information has been added to the database and tracking and monitoring continues to take place.

Task Details Period 5

Period 5 of our task order covered the tracking, monitoring, collection and submission of all tier 3 and 4 system documents (SSP, CMP, DRP/COSP) that related to the findings found during the BAH Pre-certification document reviews and recorded in each systems CAPS. On a weekly basis we contacted each of the system SSO's to determine their status as it pertained to their documents. We asked them whether they were on track to complete their remediations by the dates they provided up or whether they were having problems. We then provided that status in a weekly update to FSA's CSO on each of the systems. Those systems that had documents due during the current week were also contacted daily during the week to make sure all documents were going to be completed on time. At times wee met with them in person or discussed questions they had by phone and/or email. Once those completes documents were collected (on the days they were due) we submitted them to the Department and the CRG for review. For those systems who missed their deadlines we continued to meet and work with their SSO's daily to make sure the documents were completed and submitted soon after their missed deadlines.

During this reporting period we also updated SAIG's SSP and COS/DRP. All elements found to be deficient in SAIG's documents and provided in the CAPS were remediated. We met weekly with SAIG staff (until the documents were completed) to discuss our progress and to ask and get answers to questions as they related to SAIG's documents These two documents were completed, submitted to SAIG for review, and then provided to the Department and CRG

Task Status

This task is ongoing. We are currently waiting for the Department to provide us with the findings from the CRG. We will then provide those findings to the SSO's of those systems. We will then track those corrective actions.